International Journal of Engineering Research (ISSN : 2319-6890)
Volume No.2, Issue No.2, pp : 76-82 01 April 2013

Offline and Online E-Voting System with Embedded Security for Real Time Application

Alaguvel.R [1] and Gnanavel.G [2]

[1]Department of Electrical and Electronics Engineering, V.R.S College of Engineering&Technology, Arasur, Villupuram, Tamilnadu, India

alaguvel@engineer.com, gnanavel1982@gmail.com

***Abstract*-An electronic voting (e-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information. There are two types of e-voting: On-Line and Offline. On-line, e.g. via Internet, and offline, by using a voting machine or an electronic polling booth. Authentication of Voters, Security of voting process, Securing voted data are the main challenge of e-voting. This is the reason why designing a secure e-voting system is very important. In many proposals, the security of the system relies mainly on the black box voting machine. But security of data, privacy of the voters and the accuracy of the vote are also main aspects that have to be taken into consideration while building secure e-voting system. In this project the authenticating voters and polling data security aspects for e-voting systems was discussed. It ensures that vote casting cannot be altered by unauthorized person. The voter authentication in online e-voting process can be done by formal registration through administrators and by entering GSM One time password. In Offline e-voting process authentication can be done using facial recognization, finger vein sensing and RFID (smart cards) which enables the electronic ballot reset for allowing voters to cast their votes. Also the voted data and voters details can be sent to the nearby Database Administration unit in a timely manner using GSM System with cryptography technique.**

***Keywords*—, Facial Recognization; Fingerprint; Offline e-voting; Online e-voting; Electronic Voting**.

I INTRODUCTION

As the modern communications and Internet, today are almost accessible electronically, the computer technology users, brings the increasing need for electronic services and their security. Usages of new technology in the voting process improve the elections in natural. This new technology refers to electronic voting systems where the election data is recorded, stored and processed primarily as digital information. In the past, usually, information security was used mostly in military and government institutions. But, now need for this type of security is growing in everyday usage. In computing, e-services and information security it is necessary to ensure that data, communications or documents (electronic or physical) are enough secure and privacy enabled. Advances in cryptographic techniques allow pretty good privacy on e-voting systems.

Security is a heart of e-voting process. Therefore the necessity of designing a secure e-voting system is very important. Usually, mechanisms that ensure the security and privacy of an election can be time-consuming, expensive for election administrators, and inconvenient for voters.

There are different levels of e-voting security. Therefore serious measures must be taken to keep it out of public domain. Also, security must be applied to hide votes from publicity. There is no measurement for acceptable security level, because the level depends on type of the information. An acceptable security level is always a compromise between usability and strength of security method.

The authenticating voters and polling data security aspects for e-voting systems are discussed here. It ensures that vote casting cannot be altered by unauthorized person. The voter authentication in online e-voting process can be done by formal registration through administrators and by entering OTPCertificate. In Offline e-voting process authentication can be done using facial recognization, fingerprint sensing and RFID (smart cards) which enables the electronic ballot reset for allowing voters to cast their votes. Also the voted data and voters details can be sent to the nearby Database Administration unit in a timely manner using GSM System with cryptography technique.

The criteria are Registration through Administrator, Voter identification and verification process is done through GSM with one time password. The second Offline e-voting process includes Facial Recognization; Fingerprint sensing, RFID and Polling data processing using Cryptography Technique with RC4 Algorithm. The final process concludes the analysis of polling data in real time and immediate resulting system of e-voting system.

II ELECTRONIC VOTING SYSTEMS

An electronic voting system is a voting system in which the election data is recorded, stored and processed primarily as digital information. E-voting is referred as "electronic voting" and defined as any voting process where an electronic means is used for votes casting and results counting. E-voting is an election system that allows a voter to record their ballots in a electrically secured method. A number of electronic voting systems are used in large applications like optical scanners which read manually marked ballots to entirely electronic touch screen voting systems. Specialized voting systems like DRE (direct recording electronic) voting systems, RFID, national IDs, the Internet, computer networks, and cellular systems are also used in voting processes.

A.Securities of the E-voting systems:

The main goal of a secure e-voting is to ensure the privacy of the voters and accuracy of the votes. A secure e-voting system are satisfies the following requirements, *Eligibility*: only votes of legitimate voters shall be taken into account; *Unreusability*: each voter is allowed to cast one vote; *Anonymity*: votes are set secret; *Accuracy*: cast ballot cannot be altered. Therefore, it must not be possible to delete ballots nor to add ballots, once the election has been closed; *Fairness*: partial tabulation is impossible; *Vote and go*: once a voter has casted their vote, no further action prior to the end of the election; *Public verifiability*: anyone should be able to readily check the validity of the whole voting process.

B. Issues of Present Voting System:

There have been several studies on using computer technologies to improve elections these studies caution against the risks of moving too quickly to adopt electronic voting system, because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing. *Accuracy:* It is not possible for a vote to be altered eliminated the invalid vote cannot be counted from the finally tally .*Democracy:* It permits only eligible voters to vote and, it ensures that eligible voters vote only once. *Privacy:* Neither authority nor anyone else can link any ballot to the voter *verifiability:* Independently verification of that all votes have been counted correctly. *Resistance:* No electoral entity (any server participating in the election) or group of entities, running the election can work in a conspiracy to introduce votes or to prevent voters from voting. *Availability:* The system works properly as long as the poll stands and any voter can have access to it from the beginning to the end of the poll. *Resume Ability:* The system allows any voter to interrupt the voting process to resume it or restart it while the poll stands

The existing elections were done in traditional way, using ballot, ink and tallying the votes later. But the proposed system prevents the election from being accurate. Problems encountered during the usual elections are as follows:

- It requires human participation, in tallying the votes that makes the elections time consuming and prone to human error.
- The voter finds the event boring resulting to a small number of voters.
- Deceitful election mechanism.
- Constant spending funds for the elections staff are provided

So, the proposed electronic voting system has to be addressed with these problems.

C. Proposed system of online e-voting:

The process of voter registration before the election process is always done by Administrator as follows the before. Registration phase begins by storing the Voter information such as Unique Voter ID (11-digit number TN/99/0000012—In this, TN specifies the State, Next two digit specifies District Id and third one specifies the Unique id for each eligible voter), Name, Age, Sex, Address and District in the database, polling questions answer and GSM one time password .this condition are stratification means person has valid the polling section.

III OFFLINE E-VOTING SYSTEMS

A. Facial recognition

In this project, you will implement a face recognition system using the Principal Component Analysis (PCA) algorithm. Automatic face recognition systems try to find the identity of a given face image according to their memory. The memory of a face recognizer is generally simulated by a training set. In this project, our training set consists of the

features extracted from known face images of different persons. Thus, the task of the face recognizer is to find the most similar feature vector among the training set to the feature vector of a given test image. Here, we want to recognize the identity of a person where an image of that person (test image) is given to the system. You will use PCA as a feature extraction algorithm in this project that will be implemented is shown in Fig.1

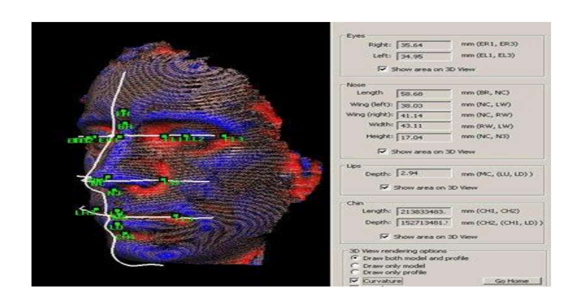


Fig 1.Facial Recognition

In the recognition phase (or, testing phase), you will be given a test image Ω_jo a known person. Let $\alpha_j$be the identity (name) of this person. As in the training phase, you should compute the feature vector of this person using PCA and obtain ω_j. In order to identify Ω_j, you should compute the similarities between $\omega_j$and all of the feature vectors ω_i's in the training set. The similarity between feature vectors can be computed using Euclidean distance. The identity of the most similar $\omega_i$will be the output of our face recognizer. If i = j, it means that we have correctly identified the person j, otherwise if i6= j , it means that we have misclassified the person j . Schematic diagram of the face recognition system that will be implemented is shown in Figure 2

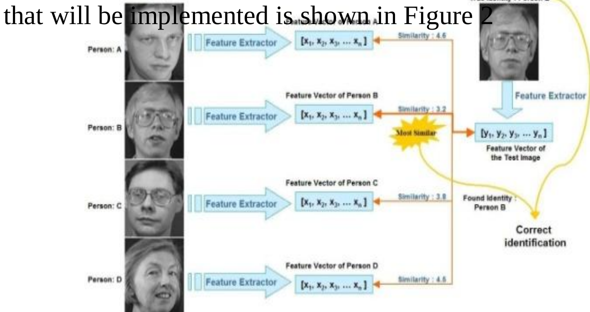


Fig. 2 Schematic diagram of a face recognizer

B. Finger Vein

Finger vein has three hardware modules: image acquisition module, ARM main board, and human machine communication module. The structure diagram of the system is shown in Fig. 1. The image acquisition module is used to collect finger-vein images. The ARM main board including the ARM chip, memory (flash), and communication port is used to execute the finger-vein recognition algorithm and communicate with the peripheral device. The human machine communication module (LED or keyboard) is used to display recognition results and receive inputs from users.

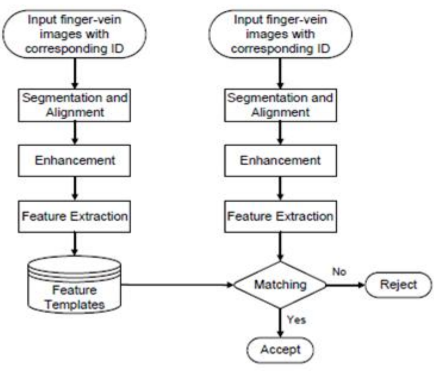


Fig.3.The flow-chart of the proposed recognition algorithm

The proposed finger-vein recognition algorithm contains two stages: the enrollment stage and the verification stage. Both stages start with finger-vein image pre-processing, which includes detection of the region of interest (ROI), image segmentation, alignment, and enhancement. For the enrollment stage, after the pre-processing and the feature extraction step, the finger-vein template database is built. For the verification stage, the input finger-vein image is matched with the corresponding template after its features are extracted. Fig. 3 shows the flow chart of the proposed algorithm. Some different methods may have been proposed for finger-vein matching. Considering the computation complexity, efficiency, and practicability, however, we propose a novel method based on the fractal theory, which will be introduced in Section 4 in detail

A. Image Acquisition:

To obtain high quality near-infrared (NIR) images, a special device was developed for acquiring the images of the finger vein without being affected by ambient temperature. Generally, finger-vein patterns can be imaged based on the principles of light reflection or light transmission. We developed a finger-vein imaging device based on light transmission for more distinct imaging.

Our device mainly includes the following modules: a monochromatic camera of resolution 580 × 600 pixels, daylight cut-off filters (lights with the wavelength less than 800 nm are cut off), transparent acryl (thickness is 10 mm),

and the NIR light source. The structure of this device is illustrated in Fig. 4. The transparent acryl serves as the platform for locating the finger and removing uneven illumination.

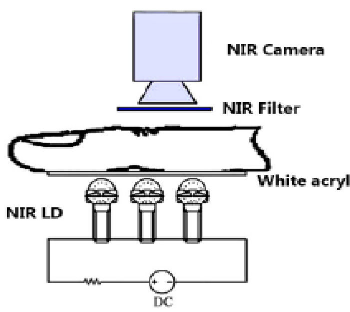


Fig.4.An example raw finger-vein image captured by our device

The NIR light irradiates the backside of the finger. In, a light-emitting diode (LED) was used as the illumination source for NIR light. With the LED illumination source, however, the shadow of the finger-vein obviously appears in the captured images. To address this problem, an NIR laser diode (LD) was used in our system. Compared with LED, LD has stronger permeability and higher power. In our device, the wavelength of LD is 808 nm. Fig. 5 shows an example raw finger-vein image captured by using our device.

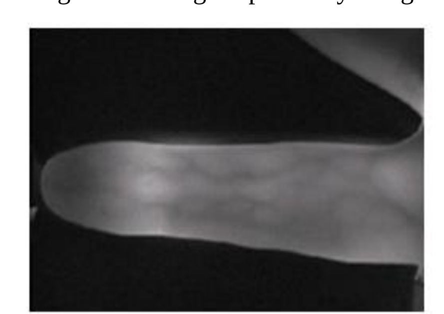


Fig.5. Illustration of the imaging device

.

IVOFFLINE E-VOTING PROCESSES

When the voter enters the voting place, he must have same kind of valid identity, which has been stored in the database for Verification. Authorized person choose to offline e-voting system. Thereare threeconditions for valid identity Verification to allow polling sectionsystem that will be implemented is shown in Figure 6

condition1: Capture the face image and compare or match to database, captured image and database image matched means that person will be valid for next condition otherwise exit the person.

Condition2: Capture the finger vein image and compare or match to database, capture finger vein and database finger vein matched means, that person will be valid for next condition otherwise exit the person..

Condition3: The voter will be verified in the electoral lists, he/she given with a “smart-card” to a "smart-card" is a card in the size and shape of a credit-card which contains a computer chip, some memory and basic data such as the voter's voting language and political party. The voter than inserts card (smart card) it into the machine .the details arecompared or matched to database. If RFID card (smart card) information and database information matched means this person will be valid for polling section and if three conditions are stratified automatically, E-voting machine buttons will be activate otherwise deactivate buttons.

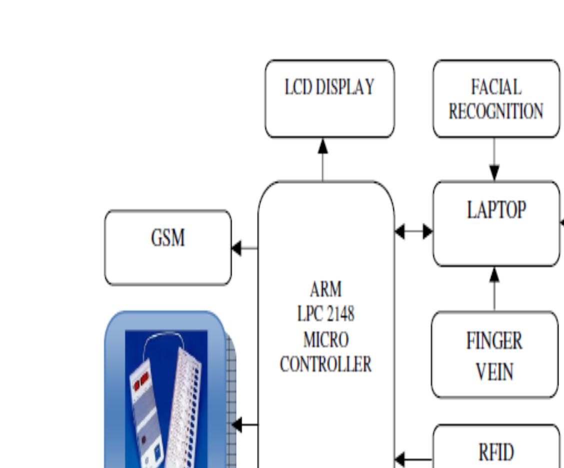


Fig.6. Offline E-Voting Block Diagram

VONLINE E -VOTING PROCESS

When the voter enters the voting place, he must have same kind of valid identity, which has been stored in database verification, authorized person choose to online e-voting system. Two conditions are verified to allow polling section.

Condition1: When a poll worker confirms that the voter is registered, login the website ,type voter ID no and password correct means go to next state, answer to polling question ,this answer correct means go to next state finger

print matched to database , matched means this person valid to next condition otherwise automatically closed web site.

Condition2: Randomly generated to one time password will be automatically sending through SMS to the authorized person's mobile device using GSM. Then authorized person type to password, if password correct means open the polling window then entered.

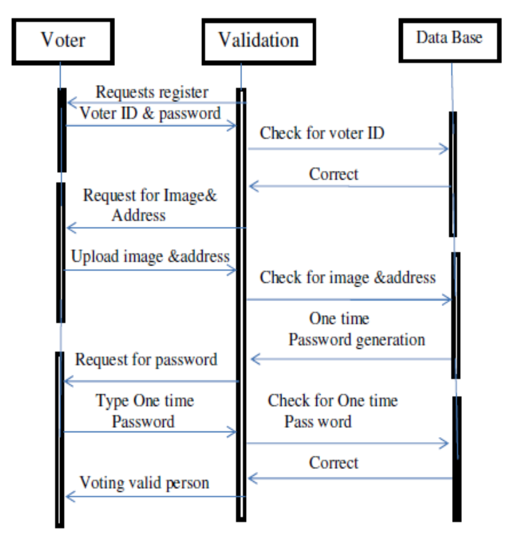


Fig.7 Authentication Sequence Diagram

VISCREEN SHORT RESULT

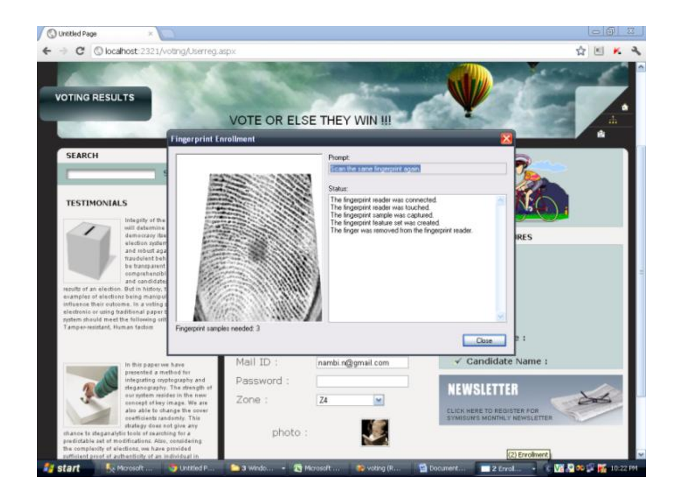


Fig.8 User Users Registration with Finger Print Enrollment

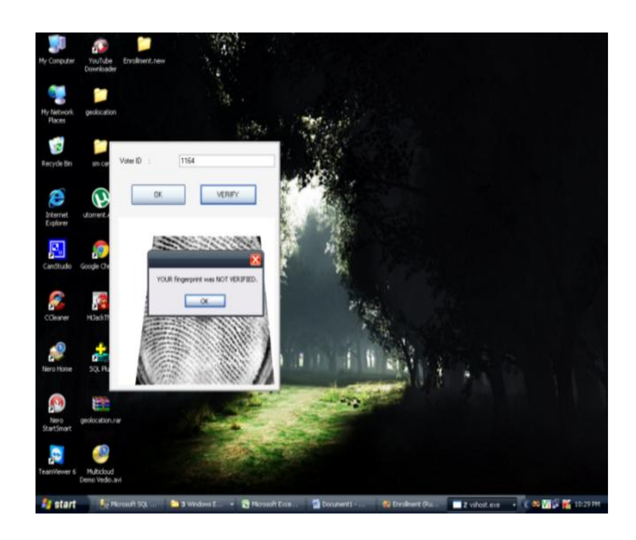


Fig.9 User login with Finger Print Verification

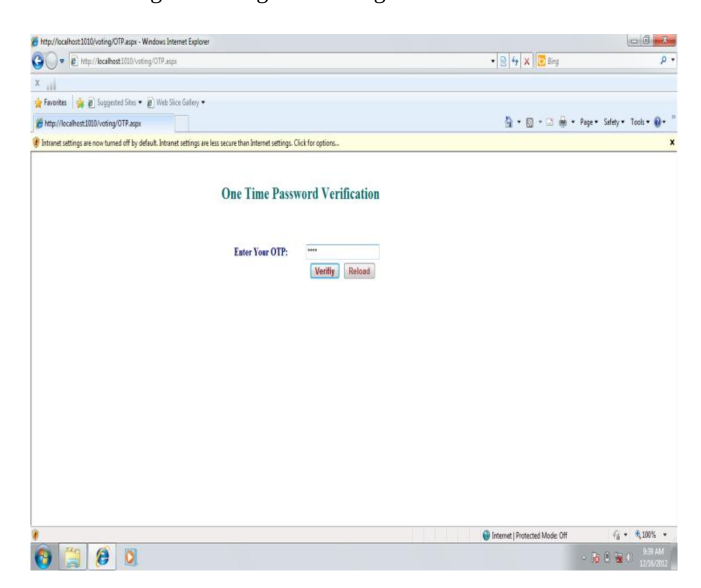


Fig.10 One Time Password



Fig.11 Online E-Voting Page

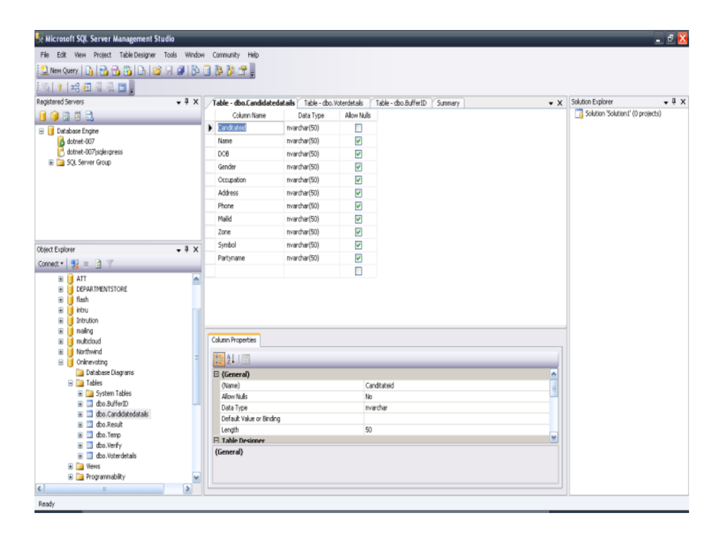


Fig.12 SQL Database Candidates Tables

VIICONCLUSION AND FUTURE ENHANCEMENT

Electronic voting systems have many advantages over the traditional way of voting. Some of these advantages are lesser cost, faster tabulation of results, improved accessibility, greater accuracy, and lower risk of human and mechanical errors. It is very difficult to design ideal e-voting system which can allow security and privacy on the high level with no compromise. Future enhancements focused to design a system which can be easy to use and will provide security and privacy of votes on acceptable level by concentrating the authentication and processing section .In case of online e-voting some authentication parameters like facial recognization, In case of offline e-voting some authentication parameters like, Finger Vein and iris matching detection can be done.

ACKNOWLEDGEMENT

We are very much grateful to **GNANAVEL.G** for whom nothing is impossible in this world & we are very much thankful that he gave opportunity to complete this work in time to us. We would also like to be very much grateful to worthy Mrs.VijayaMuthuvannan, *chairperson*,Mr.N.Muthuvannan, *director*, Mr.R.Ramanathan, *Secretary*, Er.M.Saravanan, *C.E.O*, and Dr.A.Anbalagan, Principal of V.R.S.College of Engineering & Technology.

REFERENCES

[1].Tai-Pang Wu, , Sai-Kit, Yeung,JiayaJia, Chi-Keung Tang, AndGe´ RardMedioni Closed-Form Solution To Tensor Voting:Theory And ApplicationsTransactions On Pattern Analysis And Machine Intelligence, *Vol. 34, No. 8, August 2012*

[2].Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman Attacking the Washington, D.C. Internet Voting System In Proc. *16th Conference on Financial Cryptography & Data Security, Feb. 2012*

[3].Jossy P. George Saleem S TevaramaniAnd K B RajaPerformance Comparison Of Face Recognition Using Transform Domain Techniques World *Of Computer Science And Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 3, 82-89, 2012*

[4].D. Ashok Kumar, T. UmmalSariba Begum A Novel design of Electronic Voting System Using Fingerprint *International Journal Of Innovative Technology & Creative Engineering (Issn: 2045-8711) Vol.1 No.1 January 2011*

[5].HongkaiXiong, Yang Xu,Yuan F. Zheng Wen Chen, *Fellow,* With Tensor Voting Projected Structure In Video Compression *Ieee Transactions On Circuits And Systems For Video Technology, Vol. 21, No. 8, August 2011*

[6].KashifHussainMemon, Dileep Kumar and Syed Muhammad Usman,Next Generation A Secure E-Voting System Based On Biometric Fingerprint Method *2011 International Conference On Information And Intelligent ComputingIPCSIT Vol.18 (2011)*

[7].ShivendraKatiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi Online Voting System Powered By Biometric Security Using Steganography*International Conference On Emerging Applications Of Information Technology 2011*

[8]. KalaichelviVisvalingam, R. M. ChandrasekaranSecured Electronic Voting Protocol Using Biometric Authentication

Advances In Internet Of Things, 2011 *Received June* 16, 2011; *Revised July* 5, 2011; *Accepted July* 11, 2011
[9].Feras A. Haziemeh, mutazKh. Khazaaleh, Khairall M. Al-Talafha New Applied E-Voting System *Journal Of Theoretical And Applied Information 31st March 2011*
[10].Hari K. Prasad_ J. Alex HaldermanyRopGonggrijp Scott Wolchoky Eric WustrowyArunKankipati_ Sai Krishna Sakhamuri_ VasavyaYagati_ _Netindia, Security Analysis Of India's Electronic Voting Machines *Hyderabad Y The University Of Michigan April 29, 2010*



Mr. ALAGUVEL.R, Receivedhis B.E(ECE) degree from V.R.S College of Engineering and Technology, Anna University in April 2010, has a Company experience of 1 years as a Network Engineer in Arshan Systech Pvt. Ltd., Chennai and currently pursuing his M.E (Embedded System Technologies) degree from V.R.S College of Engineering and Technology, Anna University. His areas of interest are Embedded Systems and VLSI.He presented papers in various conferences and Workshop's.



Mr. GNANAVEL.G, Received hisB.E (EEE) degree from Sri Jayaram Engineering College, Anna University in 2007, and also received his M.E (Embedded System Technologies) degree from SRM University in 2011.

Now he is working as an Assistant Professor in the Department of EEE in V.R.S College of Engineering and Technology, has a teaching experience of 7 Years. His areas of interest are Embedded Systems, Power Electronics. He presented papers in various conferences and Workshop's.